A Cipher Design with Automatic Key Generation using the Combination of Substitution and Transposition Techniques and Basic Arithmetic and Logic Operations

Govind Prasad Arya*, Aayushi Nautiyal**, Ashish Pant***, Shiv Singh**** & Tishi Handa*****

*Assistant Professor & Research Guide, Department of Computer Science & Engineering, Shivalik College of Engineering, Dehradun / Uttarakhand Technical University, Dehradun, Uttarakhand, INDIA. E-Mail: govind.arya10@gmail.com

**Research Scholar, Department of Computer Science & Engineering, Shivalik College of Engineering, Dehradun / Uttarakhand Technical University, Dehradun, Uttarakhand, INDIA. E-Mail: aayushinautiyal@gmail.com

***Research Scholar, Department of Computer Science & Engineering, Shivalik College of Engineering, Dehradun / Uttarakhand Technical University, Dehradun, Uttarakhand, INDIA. E-Mail: er.ashishpant@gmail.com

****Research Scholar, Department of Computer Science & Engineering, Shivalik College of Engineering, Dehradun / Uttarakhand Technical University, Dehradun, Uttarakhand, INDIA. E-Mail: er.shivsingh10@gmail.com

*****Research Scholar, Department of Computer Science & Engineering, Shivalik College of Engineering, Dehradun / Uttarakhand Technical University, Dehradun, Uttarakhand, INDIA. E-Mail: tishi.handa@gmail.com

***Abstract*—**Modern computing is observed to be highly dependent on communication and data transport. The security of data during communication has become a mandatory need since the introduction of e-commerce, mails, etc. Moreover a lot of data may be required to be kept secure on local devices also. The encryption of data is the basic requirement today and thus helps to maintain confidentiality of data. A number of algorithms are available for encrypting data while it is transferred from sender to receiver. In this paper we have proposed a cipher which uses basic encryption techniques of substitution and transposition along with application of logic gates, in order to encrypt the data. The algorithm makes cryptanalysis even more difficult because of the use of "Random Number Generator" function which further decides order of encryption rounds and keys to be used to encrypt the plain text. This eliminates the overhead of defining a fixed key by the user and makes algorithm secure also. It also facilitates to transfer the key to the receiver while being added with the plain text at random locations (like added at end or beginning).

***Keywords*—**Cipher, Ciphertext, Decryption, Encryption, Information Security, Key, Plaintext, Random Number, Substitution, Transposition

***Abbreviations*—**Advanced Encryption Standard (AES), American Standard Code for Information Interchange (ASCII), Data Encryption Standard (DES), Least Significant Bit (LSB)

I. INTRODUCTION

THE field of communication in computer science compels us to employ security measures since the computers are required to transfer all type of sensitive data today and their use cannot be ruled out due to its perfection, time saving and cost cutting edge. The volume of data currently transferred over the internet in a minute is about640 terabytes and it is expected that the number of devices forming network, which is nearly equal to global population, will double by 2015 [Rick Burgess, 2011]. This increment in network traffic will lead to the requirement of the ciphers which provide quick response and have low processing delay but yet are efficient.

The cipher design can be very simple as well as highly complex. Cryptology is that part of engineering which is concerned with creating ciphers (cryptography) and breaking the ciphers (cryptanalysis) [Jonathan Katz & Yehuda Lindell, 2007].

A number of ciphers are available today and are used for encryption and decryption. Some of them are block ciphers [Sastry et al., 2010], stream ciphers, and hash functions [William Stallings, 2013]. Block ciphers [Sastry et al., 2010] takes plain text input of fixed size and produces the same sized block of cipher text whereas stream cipher encrypts the stream of data i.e. one byte at a time. In this research we will mainly concentrate over the ones which use the techniques of substitution and transposition [William Stallings, 2013], using the ASCII characters [www.asciitable.com].

Substitution method [Venkateswaram & Sundaram, 2010] involves replacement of a character by another one whereas in transposition the positions of characters are changed accordingly [William Stallings, 2013]. And thus our algorithm will be a combination of these two. A number of algorithms are available today like DES [IBM, 1994] and AES [William Stallings, 2004], but none of the use the basic substitution and transposition schemes. Moreover, they execute in several rounds thereby contributing to a considerably large processing delay. Also certain algorithms using basic encryption techniques lack in automatic key generation thus contributing to overhead for users. Also these algorithms generally perform encryption by following a fixed order of rounds which can be randomized using a random number generator function [Brue Schneier, 1996].

II. SHORTCOMINGS OF PREVIOUS ALGORITHM

- The previous algorithm makes use of a fixed key initially. This fixed key is defined by the user itself which can become overhead for the user.
- The algorithm generates five keys for the five different rounds, which are the first to fifth multiple of the initial key. Therefore if the initial key is known by attacker, all the other five keys can be known.
- Since the orders in which rounds are applied in algorithm are always fixed, hence decryption becomes easy.

III. OUR CONTRIBUTION

The algorithm proposed by us uses the keys for encryption, which are generated from the message itself and are not required to be defined by the user whereas in the previous algorithm the initial key was supposed to be defined by the user explicitly [Srikantaswamy & Phaneendra, 2011]. Once the encryption is done, the key is to be transferred to the receiver's end so that it could be used for decryption. Therefore it is transferred to the receiver's end while being added with the message in the encrypted form. Another role is played by random number generator to enhance security. The algorithm uses the substitution and rail-fence technique [William Stallings, 2013] but the random number decides that which one of the two encryption techniques has to be applied first. The length of the original message decides the key to be used for substitution encryption. After this when both the algorithms have been applied, we apply NOT gate to each character. If the length of message is even, the key will be added at the end and the notation used for random number will be placed at the beginning of message in a byte else the notation will be stored at the end and key at the beginning. The notation for random number will be zero if it is even and one if it is odd. The key will also be stored in a byte using the five LSB of the word. The final message will be transmitted over the network.

The decryption algorithm on the other end will separate the key and notation used for random number from the cipher text by counting its length. Once they are separated, the cipher text will undergo NOT operation and decryption rounds will be applied subsequently, on the basis of random number notation. If random number notation is zero, rail-fence will be applied first and then substitution, else vice-versa.

IV. ENCRYPTION ALGORITHM

```
Step 1:  Generate a Random Number R.
Step 2:  If R is Even, go to Step 3.
Else: go to Step 9.
Step 3: Count the length of String
Step 4: if length is even, go to Step 5.
Else go to Step 6.
Step 5: Calculate key (K) for substitution by looking for Letter at Position n/2, Calculate a numeric Value by Considering A=1, B=2 …Z=26 and go to Step 7.
Step 6: calculate Key (K) for substitution by looking for Letter at Position (n+1)/2, Calculate a numeric Value by Considering A=1, B=2 …Z=26.
Step 7: Apply Substitution using formula C=(p+k) mod 26; where c is cipher text , p is plain text and key K.
Step 8: Apply transposition, i.e. Rail Fence Technique on result of Step 7 and go to Step 15.
Step 9: Apply rail-fence transposition to the Plain Text.
Step 10: Count the length of string.
Step 11: if length is even, go to Step 12.
    Else go to Step 13.
Step 12: Calculate key (K) for substitution by looking for Letter at Position n/2, Calculate a numeric Value by Considering A=1, B=2 …Z=26 and go to Step 14.
Step 13: calculate Key (K) for substitution by looking for Letter at Position (n+1)/2, Calculate a numeric Value by Considering A=1, B=2 …Z=26.
Step 14: Apply Substitution to the result of Step 9 using formula C=(p+k) mod 26; where c is cipher text , p is plain text and key K.
Step 15: On the transposed result, apply Logical gate NOT.
STOP
```

Final Cipher text will be the output of previous step.

V. ENCRYPTION AND DECRYPTION RESULT

Example: Consider the plaintext message "NETWORKS".

The Encryption and Decryption results produced by the Algorithm are as follows

- A Random key is generated by random function.
  Let, key generated be 102. Since the key is even, substitution technique will be applied first or else

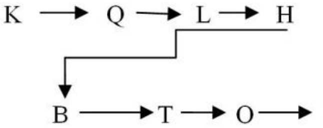
transposition technique would have been applied first.

- Now the length of original string NETWORKS is counted, which is 8. Since 8 is even number, the Key is generated using (n/2) i.e. 8/2=4 or else the key generated should be (n+1)/2).
- Now the key i.e. letter at position 4 is 'W', and key chosen will be word's corresponding numeric value i.e. k=23 (consider A=1, B=2… Z=26)

Table 1 – Encryption

Original Text	Numeric Value of English Alphabet	C = (p+k) mod 26	Corresponding English Alphabet of C
N	14	(14+23) mod 26 =11	K
E	5	(5+23) mod 26 =2	B
T	20	(20+23) mod 26 =17	Q
W	23	(23+23) mod 26 =20	T
O	15	(15+23) mod 26 =12	L
R	18	(18+23) mod 26 =15	O
K	11	(11+23) mod 26 =8	H
S	19	(19+23) mod 26 =16	P

After round 1 of encryption, we get KBQTLOHP. Apply transposition i.e. Rail Fence.



Cipher Text= KQLHBTOP

In final Round of Encryption, apply Logical Gate 'NOT'.

Table 2 – Encryption

Original Text	ASCII Value	Binary Equivalent	NOT	Decimal Equivalent	ASCII Equivalent in Character
K	75	01001011	10110100	180	-|
Q	81	01010001	10101110	174	«
L	76	01001100	10110011	179	|
H	72	01001000	10110111	183	Π
B	66	01000010	10111101	189	٧
T	84	01010100	10101011	171	½
O	79	01001111	10110000	168	¿
P	80	01010000	10101111	175	»

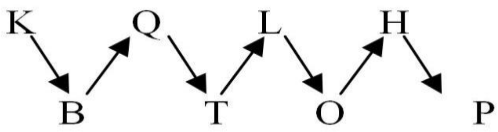
Final Cipher Text	-|	«	|	Π	٧	½	¿	»

Table 3 – Decryption

	ASCII Value in Decimal	ASCII's Binary Equivalent	NOT	Decimal Equivalent	ASCII Equivalent in Character
-|	180	10110100(180)	01001011	75	K
«	174	10101110(174)	01010001	81	Q
|	179	10110011(179)	01001100	76	L
Π	183	10110111(183)	01001000	72	H
٧	189	10111101(189)	01000010	66	B
½	171	10101011(171)	01010100	84	T
¿	168	10110000(168)	01001111	79	O
»	175	10101111(175)	01010000	80	P

Text Obtained – KQLHBTOP

Apply Reverse Transposition as:-



Text Obtained: - KBQTLOHP

Key used in Encryption, k=23

Table 4 – Decryption

	Numeric Value of English Alphabet	P=|c-k| mod 26	Corresponding Alphabet in English
K	11	|11-23|mod 26=14	N
B	2	|2-23| mod 26=5	E
Q	17	|17-23| mod 26=20	T
T	20	|20-23| mod 26=23	W
L	12	|12-23| mod 26=15	O
O	15	|15-23| mod 26=18	R
H	8	|8-23| mod 26=11	K
P	16	|16-23| mod 26=19	S

VI. Advantages of Algorithm

- Less time complexity
- Easy to understand and implement program
- Uses basic and easy encryption schemes
- Efficient key generation technique

VII. Conclusion

The main aim of encryption is to convert the text into such a form that its crypt analysis becomes tedious and confusing. The algorithm provides good encryption and is automated. The keys used are very random and cannot be identified. And all this is achieved with simple and compact code which does not lead to large processing delay and time complexity. In future the algorithm can also be applied to the Digital Image Processing and can be used to distort an image file and on the other hand the original picture can be retained. The algorithm can also be applied to the numeric data in future.

References

[1] IBM (1994), "The Data Encryption Standard (DES) and its Strength against Attacks", *IBM Journal of research and Development*, Vol. 38, Pp. 243–250.

[2] Brue Schneier (1996), "Applied Cryptography Protocols, Algorithms and Source Coding", *John Wiley & Sons, Inc.*, Second Edition.

[3] William Stallings (2004). "Network Security Essentials (Applications and Standards)", *Pearson Education*, Pp. 2–80.

[4] Jonathan Katz & Yehuda Lindell (2007), "Introduction to Modern Cryptography: Principles and Protocols", *Chapman & Hall/CRC Cryptography and Network Security Series*.

[5] V.U.K. Sastry, D.S.R. Murthy & Dr. S. Durga Bhavani (2010), "A Block Cipher having a Key on One Side of Plaintext Matrix and its Inverse on the other side", *International Journal of Computer Theory and Engineering*, Vol. 2, No. 5, Pp. 805–808.

[6] R. Venkateswaram & Dr.V. Sundaram (2010), "Information Security: Text Encryption and Decryption with Poly Substitution Method and Combining Features of Cryptography", *International Journal of Computer Applications*, Vol. 3, No. 7, Pp. 28–31.

[7] S.G. Srikantaswamy & H.D. Phaneendra (2011), "A Cipher Design using the Combined Effect of Arithmetic and Logic Operations with Substitutions and Transposition Techniques", *International Journal of Computer Applications*, Vol. 29, No. 8, Pp. 34–36.

[8] Rick Burgess (2011), URL: "http://www.techspot.com / 52011-one-minute-on-the-internet-640tb-data-transferred-100k-tweets-204-million-e-mails-sent.html"

[9] William Stallings (2013), "Cryptography & Network Security: Principles & Practice", *Pearson Education*, 5th Edition.

[10] URL: "www.asciitable.com"

Govind Prasad Arya has completed Master of Technology (M.Tech) in Computer Science & Engineering from Uttarakhand Technical University. He has 8 years of teaching experience from different institutions (Govt. Polytechnic Dwarahat, Kumaon Engineering College Dwarahat). Presently he is working at Shivalik College of Engineering, as an Assistant Professor in Computer Science & Engineering Department. Data Structures, Computer Organization, Operating System & Compiler Design are his area of interest. His two research papers on DNA Compression have been published by reputed International Journals. He has attended 4 conferences and 6 seminars.

Aayushi Nautiyal is a final year student and is pursuing B.Tech in Computer Science and Engineering branch from Shivalik College of Engineering which is affiliated from Uttarakhand Technical University. Her final year project is design of a cipher using basic encryption schemes. She has attended Linux workshop under the "Spoken Tutorial" and "Talk To A Teacher" projects of IIT Bombay, funded by National Mission on Education through ITC and Human Resource and Development (HRD), Govt. of India and qualified their online examination. She has published 2 research papers till now in IJRFE.

Ashish Pant is a final year B.Tech student in Computer Science and Engineering branch from Shivalik College of Engineering which is affiliated from Uttarakhand Technical University. His final year project is design of a cipher using basic encryption schemes. He has worked upon a PHP project on Job Portal. He has attended Linux workshop under the "Spoken Tutorial" and "Talk To A Teacher" projects of IIT Bombay, funded by National Mission on Education through ITC and HRD, Govt. of India and qualified their online examination.

Shiv Singh is a final year student and is pursuing B.Tech in Computer Science and Engineering branch from Shivalik College of Engineering which is affiliated from Uttarakhand Technical University. His final year project is design of a cipher using basic encryption schemes. He has attended Seminar on Ethical Hacking from KYRON GROUP affiliated by IIT-Kharagpur. I have worked upon projects on PHP also like Blood Bank Management System.

Tishi Handa is a final year B.Tech student in Computer Science and Engineering branch from Shivalik College of Engineering which is affiliated from Uttarakhand Technical University. Her final year project is design of a cipher using basic encryption schemes. She has worked upon blood bank management system PHP project & attended ethical hacking seminar certified by IIT Kharagpur.